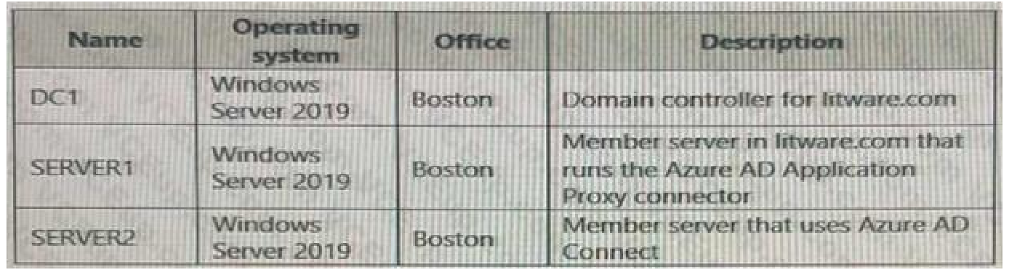
Microsoft.Premium.SC-300.20q

Number: SC-300
Passing Score: 800
Time Limit: 120 min

Exam Code: SC-300
Exam Name: Microsoft Identity and Access Administrator
Certification Provider: Microsoft
Corresponding Certification: Microsoft Certified: Identity and Access Administrator Associate
Website: https://VCEup.com/

Topic 01

QUESTION 1
Litware, Inc
Overview
Litware, Inc. is a pharmaceutical company that has a subsidiary named fabrikam, inc Litware has offices in Boston and Seattle, but has employees located across the United States.
Employees connect remotely to either office by using a VPN connection.
Identity Environment
The network contains an Active Directory forest named litware.com that is linked to an Azure Active Directory (Azure AD) tenant named litware.com. Azure AD Connect uses pass-through authentication and has password hash synchronization disabled.
Litware.com contains a user named User1 who oversees all application development. Litware implements Azure AD Application Proxy.
Fabrikam has an Azure AD tenant named fabrikam.com. The users at Fabrikam access the resources in litware.com by using guest accounts in the litware.com tenant.
Cloud Environment
All the users at Litware have Microsoft 365 Enterprise E5 licenses. All the built-in anomaly detection polices in Microsoft Cloud App Security are enabled.
Litware has an Azure subscription associated to the litware.com Azure AD tenant. The subscription contains an Azure Sentinel instance that uses the Azure Active Directory connector and the Office 365 connector. Azure Sentinel currently collects the Azure AD sign-ins logs and audit logs.
On-premises Environment
The on-premises network contains the severs shown in the following table.



Name	Operating system	Office	Description
DC1	Windows Server 2019	Boston	Domain controller for litware.com
SERVER1	Windows Server 2019	Boston	Member server in litware.com that runs the Azure AD Application Proxy connector
SERVER2	Windows Server 2019	Boston	Member server that uses Azure AD Connect

Both Litware offices connect directly to the internet. Both offices connect to virtual networks in the Azure subscription by using a site-to-site VPN connection. All on-premises domain controllers are prevented from accessing the internet.
Delegation Requirements
Litware identifies the following delegation requirements:
* Delegate the management of privileged roles by using Azure AD Privileged Identity Management (PIM).
* Prevent nonprivileged users from registering applications in the litware.com Azure AD tenant- * Use custom catalogs and custom programs for Identity Governance.
* Ensure that User1 can create enterprise applications in Azure AD. Use the principle of least privilege.
Licensing Requirements
Litware recently added a custom user attribute named LWLicenses to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the LWLicenses attribute. Users who have the appropriate value for LWLicenses must be added automatically to Microsoft 365 group that he appropriate license assigned.
Management Requirement
Litware wants to create a group named LWGroup1 will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Authentication Requirements
Litware identifies the following authentication requirements:
• Implement multi-factor authentication (MFA) for all Litware users.
• Exempt users from using MFA to authenticate to Azure AD from the Boston office of Litware.
• Implement a banned password list for the litware.com forest.
• Enforce MFA when accessing on-premises applications.
• Automatically detect and remediate externally leaked credentials
Access Requirements
Litware wants to create a group named LWGroup1 that will contain all the Azure AD user accounts for Litware but exclude all the Azure AD guest accounts.
Monitoring Requirements
Litware wants to use the Fusion rule in Azure Sentinel to detect multi-staged that include a combination of suspicious Azure AD sign-ins followed by anomalous Microsoft Office 365 activity.

A.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
You need to configure the MFA settings for users who connect from the Boston office. The solution must meet the authentication requirements and the access requirements.
What should you configure?

A. named locations that have a private IP address range
B. named locations that have a public IP address range
C. trusted IPs that have a public IP address range
D. trusted IPs that have a private IP address range

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-conditionLocation offer your country set, IP ranges MFA trusted IP and corporate network VPN gateway IP address: This is the public IP address of the VPN device for your on-premises network. The VPN device requires an IPv4 public IP address. Specify a valid public IP address for the VPN device to which you want to connect. It must be reachable by Azure Client Address space: List the IP address ranges that you want routed to the local on-premises network through this gateway. You can add multiple address space ranges. Make sure that the ranges you specify here do not overlap with ranges of other networks your virtual network connects to, or with the address ranges of the virtual network itself.

QUESTION 3
You need to configure the detection of multi staged attacks to meet the monitoring requirements.
What should you do?

A. Customize the Azure Sentinel rule logic.
B. Create a workbook.
C. Add an Azure Sentinel playbook.
D. Add Azure Sentinel data connectors.

Correct Answer: D
Section: (none)
Explanation

Explanation/Reference:

QUESTION 4
You need to configure the detection of multi-staged attacks to meet the monitoring requirements.
What should you do?

A. Customize the Azure Sentinel rule logic.
B. Create a workbook.
C. Add Azure Sentinel data connectors.
D. Add an Azure Sentinel playbook.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 5
You need to track application access assignments by using Identity Governance. The solution must meet the delegation requirements.
What should you do first?

A. Modify the User consent settings for the enterprise applications.
B. Create a catalog.
C. Create a program.
D. Modify the Admin consent requests settings for the enterprise applications.

Correct Answer: B

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-managementoverview

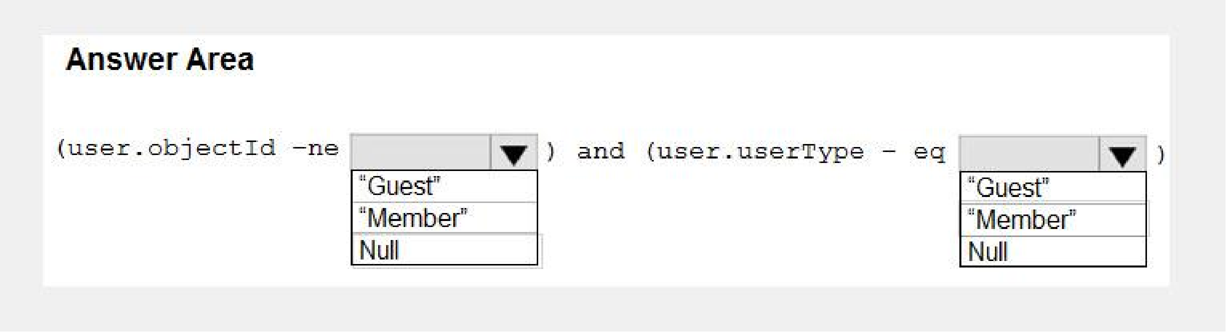
QUESTION 6
HOTSPOT

You need to create the LWGroup1 group to meet the management requirements.

How should you complete the dynamic membership rule? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

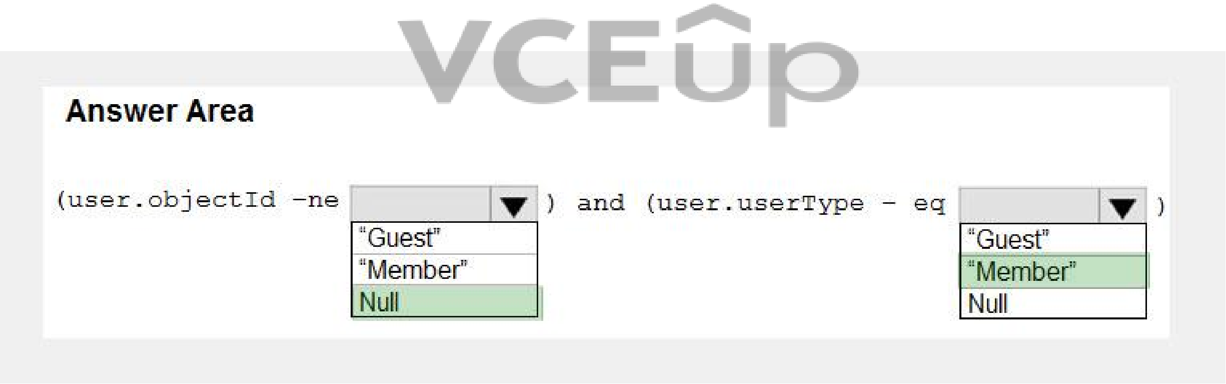


Answer Area

(user.objectId –ne ▼) and (user.userType – eq ▼)

- First list: “Guest” / “Member” / Null
- Second list: “Guest” / “Member” / Null

Correct Answer:



Answer Area

(user.objectId –ne ▼) and (user.userType – eq ▼)

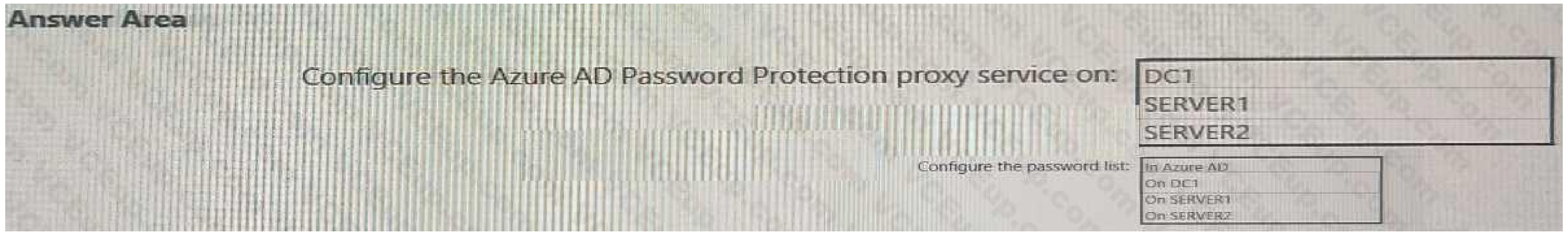
- First list: “Guest” / “Member” / [✓ Null]
- Second list: “Guest” / [✓ “Member”] / Null

Section: (none)
Explanation

Explanation/Reference:

QUESTION 7
HOTSPOT
You need to implement password restrictions to meet the authentication requirements.
You install the Azure AD password Protection DC agent on DC1.
What should you do next? To answer, select the appropriate options in the answer area.
NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

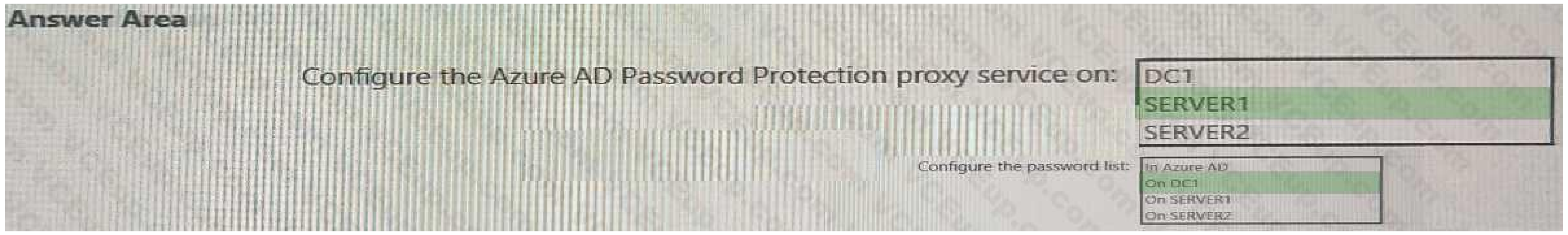
Configure the Azure AD Password Protection proxy service on:

- DC1
- SERVER1
- SERVER2

Configure the password list:

- In Azure AD
- On DC1
- On SERVER1
- On SERVER2

Correct Answer:



Answer Area

Configure the Azure AD Password Protection proxy service on:

- DC1
- [✓ SERVER1]
- SERVER2

Configure the password list:

- In Azure AD
- [✓ On DC1]
- On SERVER1
- On SERVER2

Section: (none)
Explanation

Explanation/Reference:

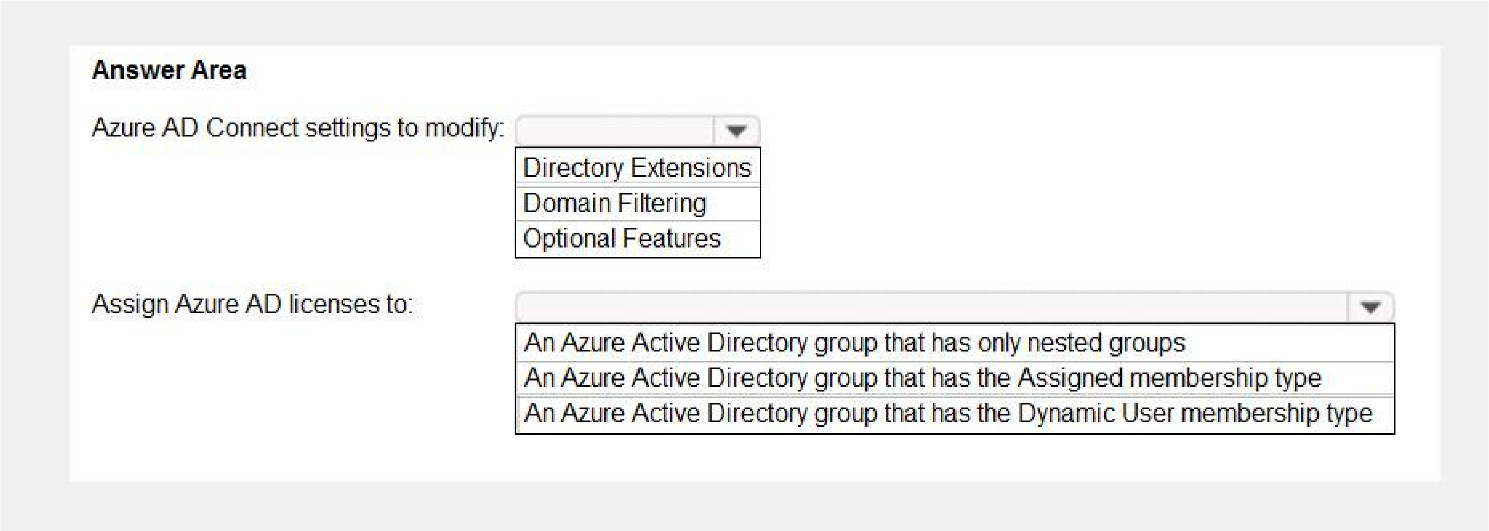
QUESTION 8
HOTSPOT

You need to configure the assignment of Azure AD licenses to the Litware users. The solution must meet the licensing requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

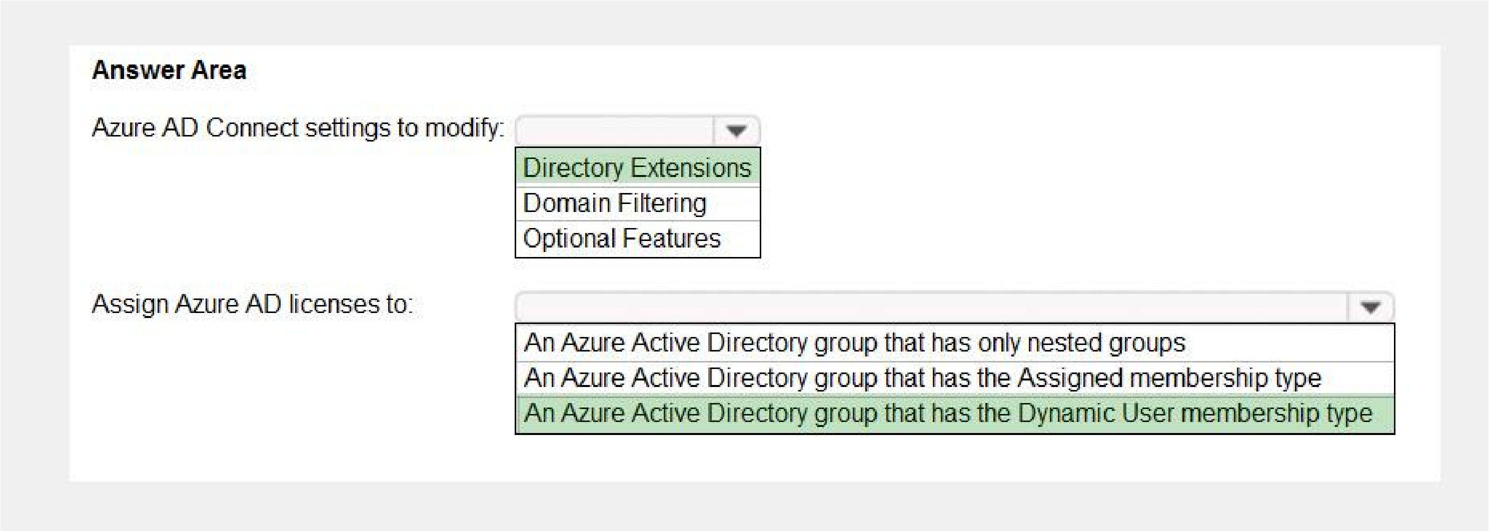
Azure AD Connect settings to modify:

- Directory Extensions
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:

- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- An Azure Active Directory group that has the Dynamic User membership type

Correct Answer:



Answer Area

Azure AD Connect settings to modify:
- [✓ Directory Extensions]
- Domain Filtering
- Optional Features

Assign Azure AD licenses to:
- An Azure Active Directory group that has only nested groups
- An Azure Active Directory group that has the Assigned membership type
- [✓ An Azure Active Directory group that has the Dynamic User membership type]

Section: (none)
Explanation

Explanation/Reference:
Explanation:

Litware recently added a custom user attribute named `LWLicenses` to the litware.com Active Directory forest. Litware wants to manage the assignment of Azure AD licenses by modifying the value of the `LWLicenses` attribute. Users who have the appropriate value for `LWLicenses` must be added automatically to a Microsoft 365 group that has the appropriate licenses assigned.

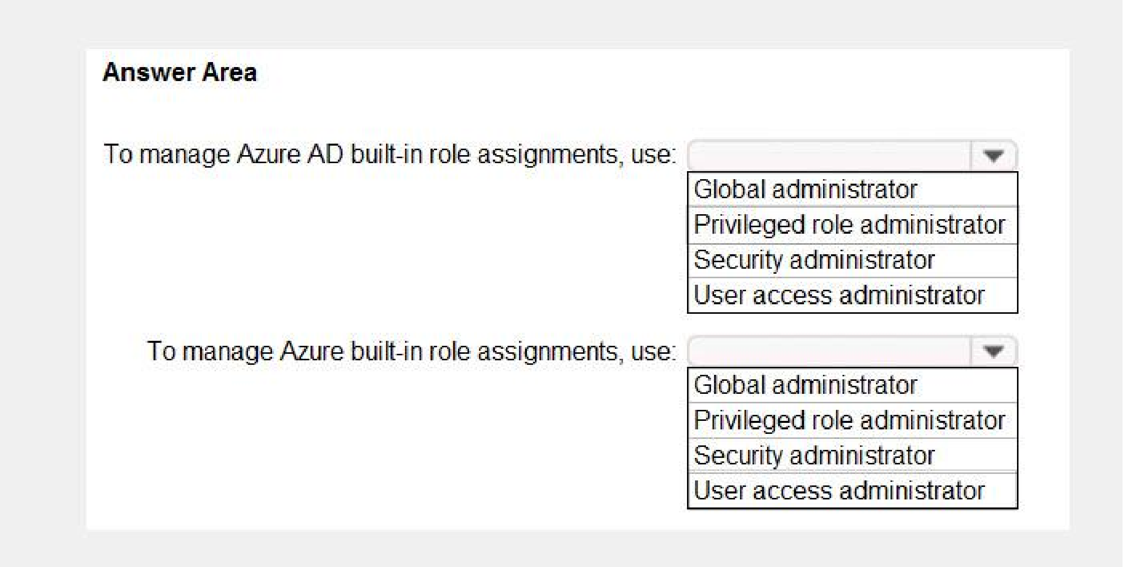
QUESTION 9
HOTSPOT

You need to identify which roles to use for managing role assignments. The solution must meet the delegation requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:

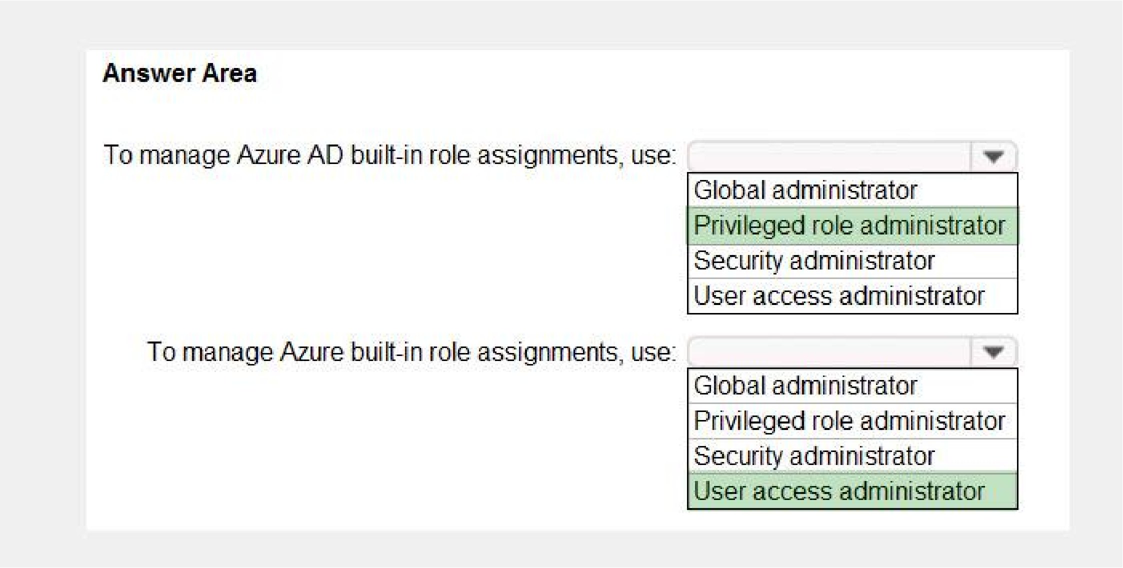


Answer Area

To manage Azure AD built-in role assignments, use:
- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

To manage Azure built-in role assignments, use:
- Global administrator
- Privileged role administrator
- Security administrator
- User access administrator

Correct Answer:



Answer Area

To manage Azure AD built-in role assignments, use:

- Global administrator
- [✓ Privileged role administrator]
- Security administrator
- User access administrator

To manage Azure built-in role assignments, use:

- Global administrator
- Privileged role administrator
- Security administrator
- [✓ User access administrator]

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/role-based-access-control/role-assignments-portal

https://docs.microsoft.com/en-us/azure/active-directory/roles/permissions-reference

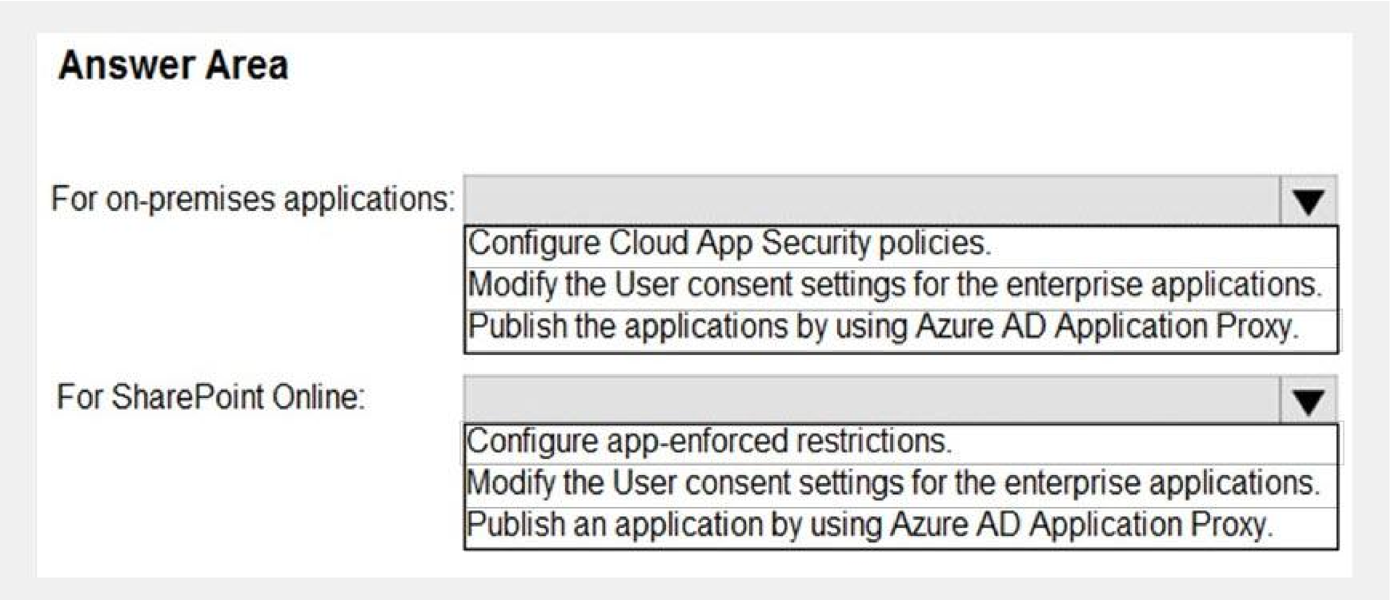
QUESTION 10
HOTSPOT

You need to implement on-premises application and SharePoint Online restrictions to meet the authentication requirements and the access requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

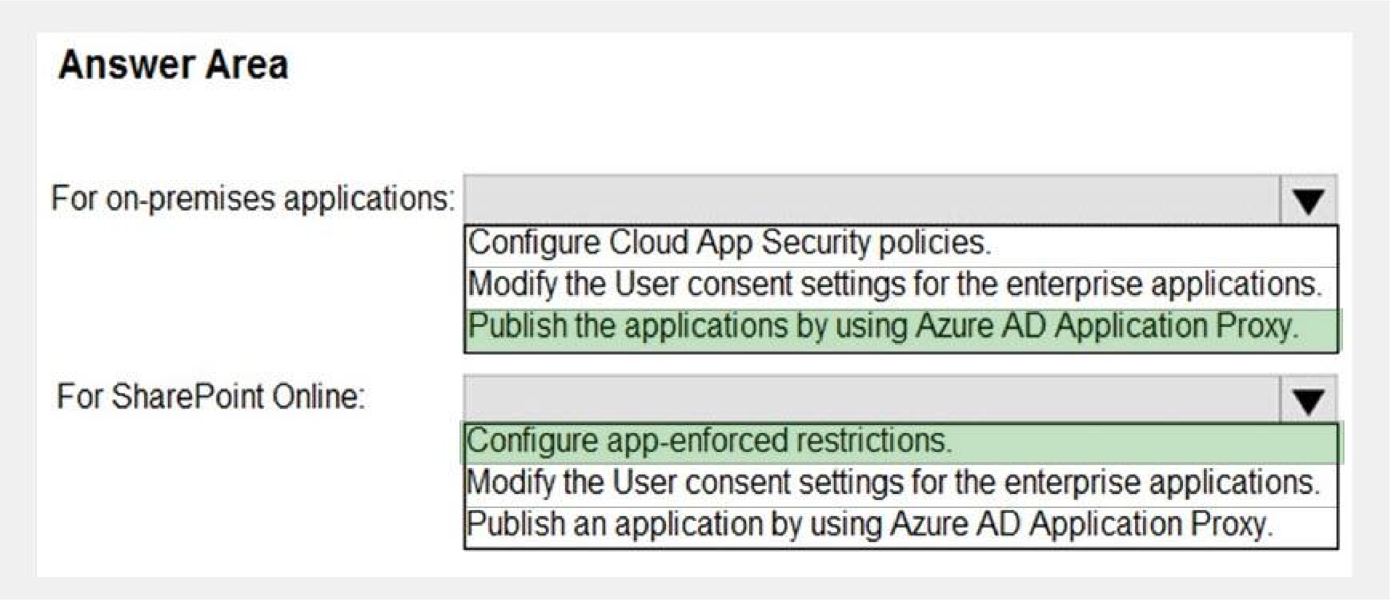
For on-premises applications:

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- Publish the applications by using Azure AD Application Proxy.

For SharePoint Online:

- Configure app-enforced restrictions.
- Modify the User consent settings for the enterprise applications.
- Publish an application by using Azure AD Application Proxy.

Correct Answer:



Answer Area

For on-premises applications:

- Configure Cloud App Security policies.
- Modify the User consent settings for the enterprise applications.
- [✓ Publish the applications by using Azure AD Application Proxy.]

For SharePoint Online:

- [✓ Configure app-enforced restrictions.]
- Modify the User consent settings for the enterprise applications.
- Publish an application by using Azure AD Application Proxy.

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/sharepoint/app-enforced-restrictions
https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-session

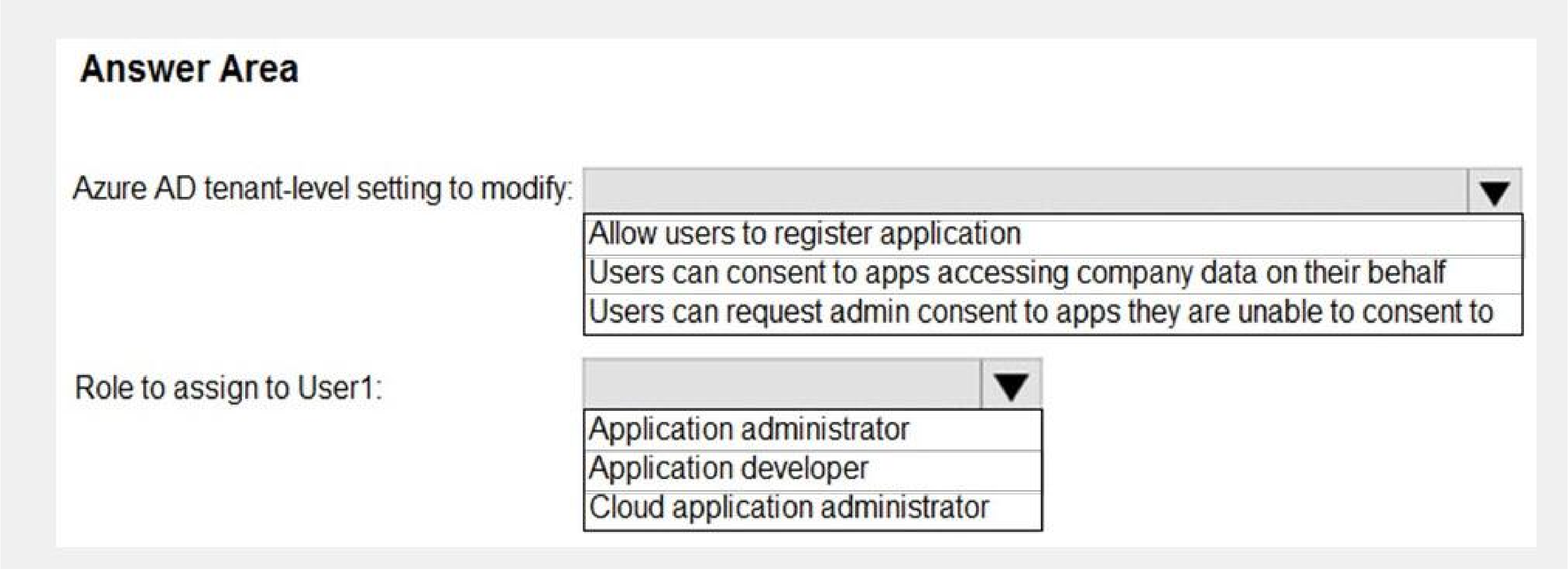
QUESTION 11
HOTSPOT

You need to configure app registration in Azure AD to meet the delegation requirements.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

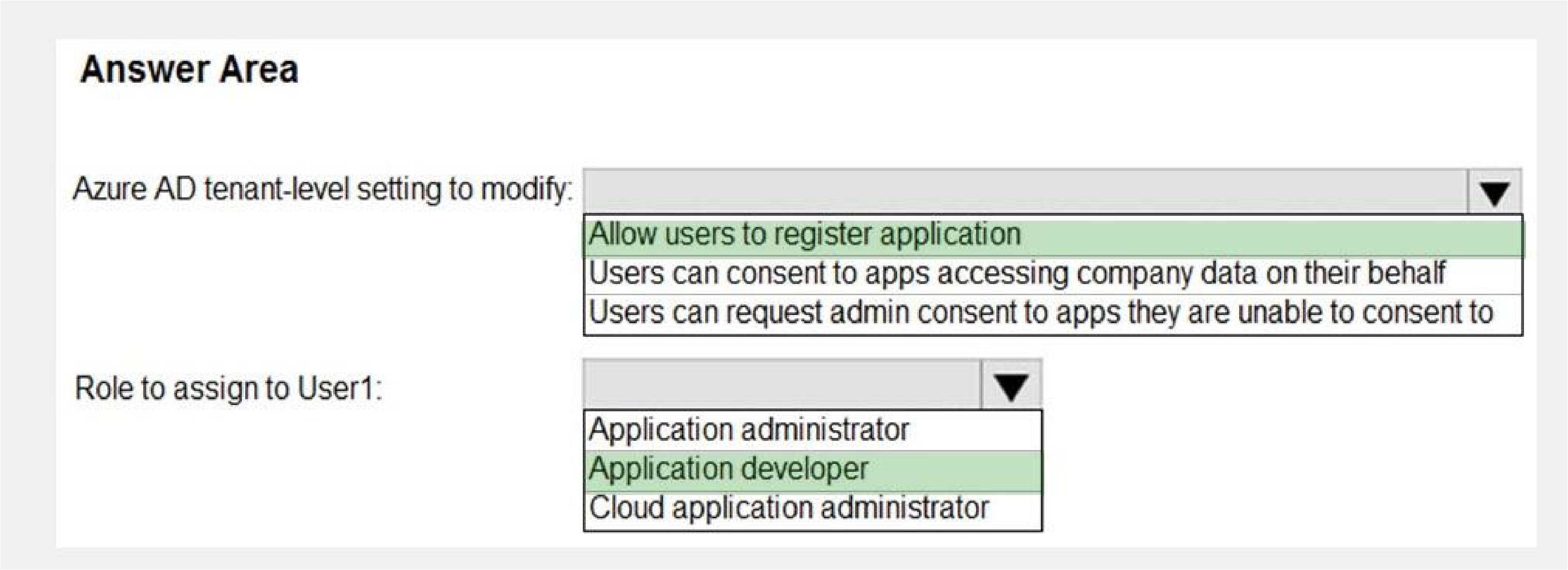
Azure AD tenant-level setting to modify:

- Allow users to register application
- Users can consent to apps accessing company data on their behalf
- Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

- Application administrator
- Application developer
- Cloud application administrator

Correct Answer:



Answer Area

Azure AD tenant-level setting to modify:

- [✓ Allow users to register application]
- Users can consent to apps accessing company data on their behalf
- Users can request admin consent to apps they are unable to consent to

Role to assign to User1:

- Application administrator
- [✓ Application developer]
- Cloud application administrator

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles

Topic 02

QUESTION 1

Contoso, Ltd

Overview

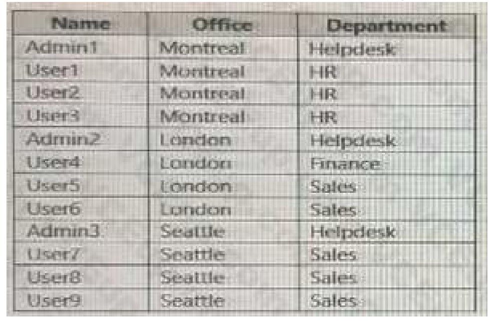
Contoso, Ltd is a consulting company that has a main office in Montreal offices in London and Seattle.

Contoso has a partnership with a company named Fabrikam, Inc Fabcricam has an Azure Active Diretory (Azure AD) tenant named fabrikam.com.

Existing Environment

The on-premises network of Contoso contains an Active Directory domain named contos.com. The domain contains an organizational unit (OU) named Contoso_Resources. The Contoso_Resoureces OU contains all users and computers.

The Contoso.com Active Directory domain contains the users shown in the following table.



Name	Office	Department
Admin1	Montreal	Helpdesk
User1	Montreal	HR
User2	Montreal	HR
User3	Montreal	HR
Admin2	London	Helpdesk
User4	London	Finance
User5	London	Sales
User6	London	Sales
Admin3	Seattle	Helpdesk
User7	Seattle	Sales
User8	Seattle	Sales
User9	Seattle	Sales

Microsoft 365/Azure Environment

Contoso has an Azure AD tenant named Contoso.com that has the following associated licenses:

Microsoft Office 365 Enterprise E5

Enterprise Mobility + Security

Windows 10 Enterprise E5

Project Plan 3

Azure AD Connect is configured between azure AD and Active Directory Domain Serverless (AD DS).

Only the Contoso Resources OU is synced.

Helpdesk administrators routinely use the Microsoft 365 admin center to manage user settings.

User administrators currently use the Microsoft 365 admin center to manually assign licenses, All user have all licenses assigned besides following exception:

The users in the London office have the Microsoft 365 admin center to manually assign licenses. All user have licenses assigned besides the following exceptions:

The users in the London office have the Microsoft 365 Phone System License unassigned.

The users in the Seattle office have the Yammer Enterprise License unassigned.

Security defaults are disabled for Contoso.com.

Contoso uses Azure AD Privileged identity Management (PIM) to project administrator roles.

Problem Statements

Contoso identifies the following issues:

- Currently, all the helpdesk administrators can manage user licenses throughout the entire Microsoft 365 tenant.
- The user administrators report that it is tedious to manually configure the different license requirements for each Contoso office.
- The helpdesk administrators spend too much time provisioning internal and guest access to the required Microsoft 365 services and apps.
- Currently, the helpdesk administrators can perform tasks by using the: User administrator role without justification or approval.
- When the Logs node is selected in Azure AD, an error message appears stating that Log Analytics integration is not enabled.

Planned Changes

Contoso plans to implement the following changes.

Implement self-service password reset (SSPR). Analyze Azure audit activity logs by using Azure Monitor-Simplify license allocation for new users added to the tenant. Collaborate with the users at Fabrikam on a joint marketing campaign.

Configure the User administrator role to require justification and approval to activate.

Implement a custom line-of-business Azure web app named App1. App1 will be accessible from the internet and authenticated by using Azure AD accounts.

For new users in the marketing department, implement an automated approval workflow to provide access to a Microsoft SharePoint Online site, group, and app.

Contoso plans to acquire a company named Corporation. One hundred new A Datum users will be created in an Active Directory OU named Adatum. The users will be located in London and Seattle.

Technical Requirements

Contoso identifies the following technical requirements:

- AH users must be synced from AD DS to the contoso.com Azure AD tenant.
- App1 must have a redirect URI pointed to https://contoso.com/auth-response.
- License allocation for new users must be assigned automatically based on the location of the user.
- Fabrikam users must have access to the marketing department's SharePoint site for a maximum of 90 days.
- Administrative actions performed in Azure AD must be audited. Audit logs must be retained for one year.
- The helpdesk administrators must be able to manage licenses for only the users in their respective office.
- Users must be forced to change their password if there is a probability that the users' identity was compromised.

A.

B.

C.

D.

Correct Answer:
Section: (none)
Explanation

Explanation/Reference:

QUESTION 2
You need to locate licenses to the

A. Datum users. The solution must need the technical requirements.
Which type of object should you create?
B. A Dynamo User security group
C. An OU
D. A distribution group
E. An administrative unit

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:

QUESTION 3
You need to meet the planned changes for the User administrator role.
What should you do?

A. Create an access review.
B. Modify Role settings
C. Create an administrator unit.
D. Modify Active Assignments.

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Role Setting details is where you need to be: Role setting details - User Administrator Privileged Identity Management | Azure AD roles Default Setting State Require justification on activation Yes Require ticket information on activation No On activation, require Azure MFA Yes Require approval to activate No Approvers None

QUESTION 4
You need to sync the ADatum users. The solution must meet the technical requirements.
What should you do?

A. From the Microsoft Azure Active Directory Connect wizard, select Customize synchronization options.
B. From PowerShell, run Set-ADSyncScheduler.
C. From PowerShell, run Start-ADSyncSyncCycle.
D. From the Microsoft Azure Active Directory Connect wizard, select Change user sign-in.

Correct Answer: A
Section: (none)
Explanation

Explanation/Reference:
Explanation:
You need to select Customize synchronization options to configure Azure AD Connect to sync the Adatum organizational unit (OU).

QUESTION 5
You need to meet the planned changes and technical requirements for App1.
What should you implement?

A. a policy set in Microsoft Endpoint Manager
B. an app configuration policy in Microsoft Endpoint Manager
C. an app registration in Azure AD
D. Azure AD Application Proxy

Correct Answer: C
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app

QUESTION 6
You create a Log Analytics workspace.
You need to implement the technical requirements for auditing.
What should you configure in Azure AD?

A. Company branding
B. Diagnostics settings
C. External Identities
D. App registrations

Correct Answer: B
Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/overview-monitoring

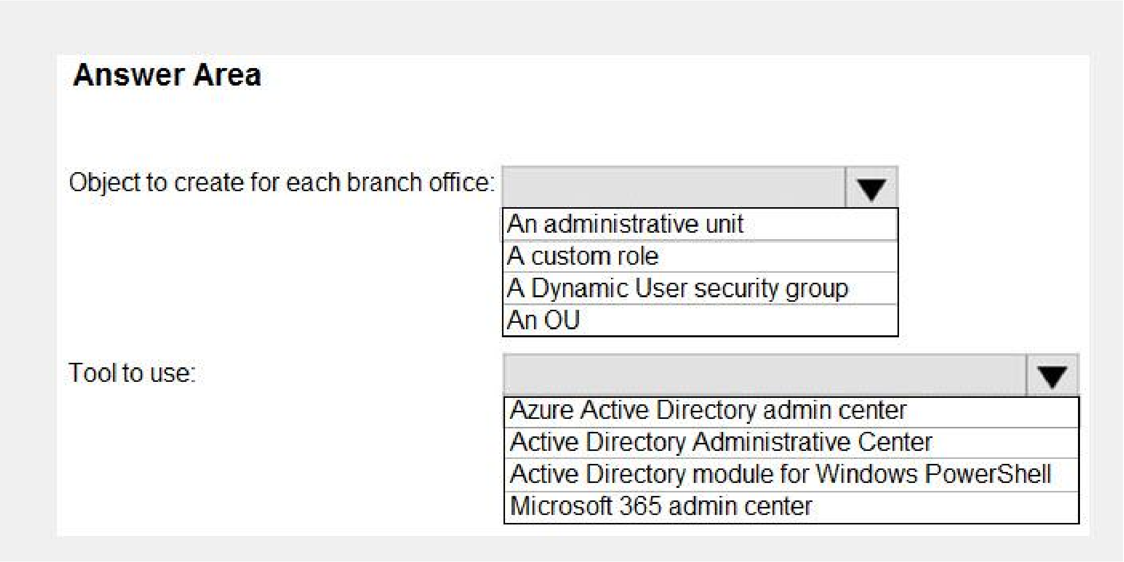
QUESTION 7
HOTSPOT

You need to meet the technical requirements for license management by the helpdesk administrators.

What should you create first, and which tool should you use? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

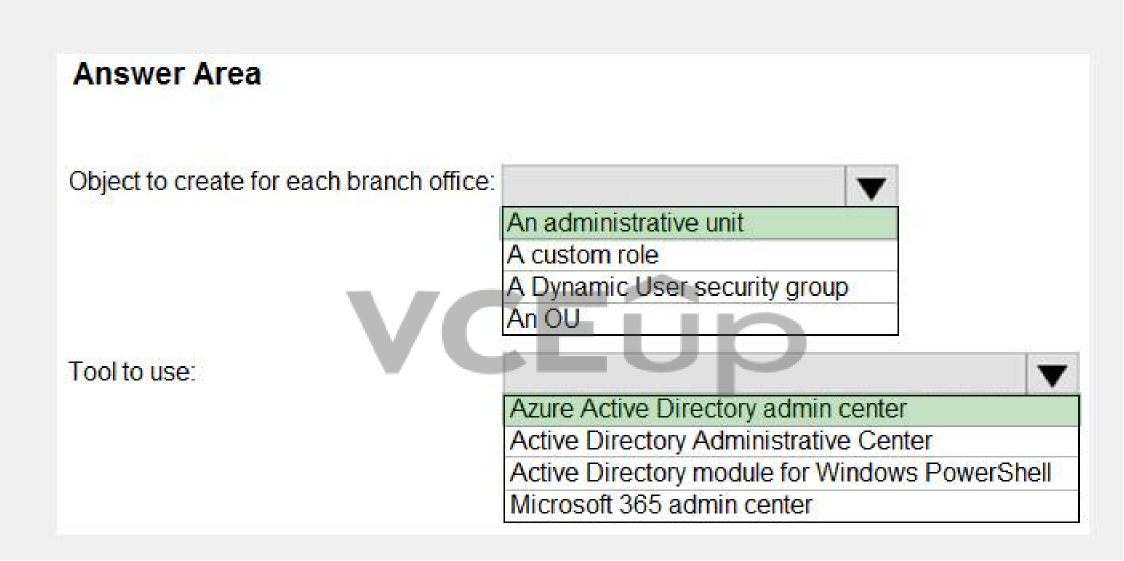
Object to create for each branch office:

- An administrative unit
- A custom role
- A Dynamic User security group
- An OU

Tool to use:

- Azure Active Directory admin center
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Correct Answer:



Answer Area

Object to create for each branch office:

- [✓ An administrative unit]
- A custom role
- A Dynamic User security group
- An OU

Tool to use:

- [✓ Azure Active Directory admin center]
- Active Directory Administrative Center
- Active Directory module for Windows PowerShell
- Microsoft 365 admin center

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/roles/administrative-units

https://docs.microsoft.com/en-us/azure/active-directory/roles/admin-units-manage

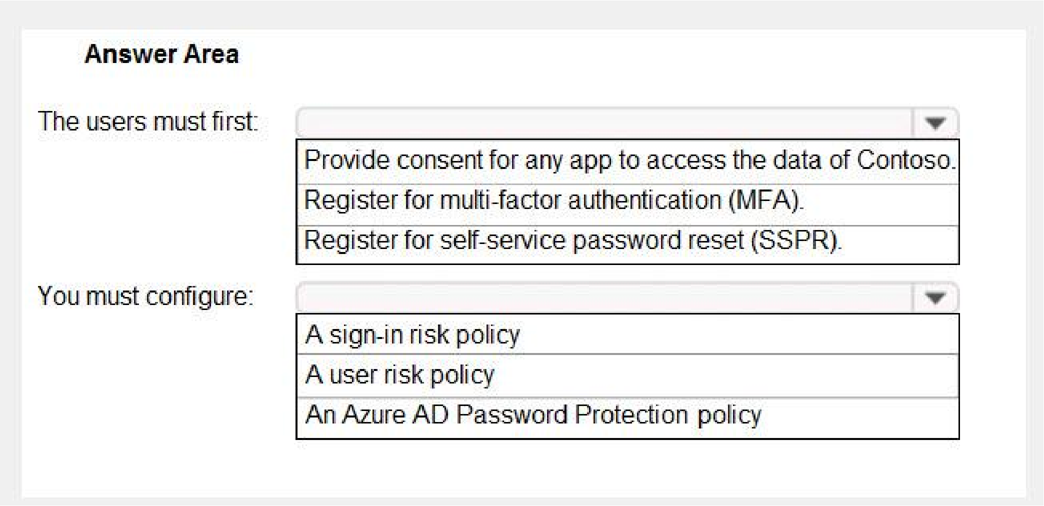
QUESTION 8
HOTSPOT

You need to meet the technical requirements for the probability that user identities were compromised.

What should the users do first, and what should you configure? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

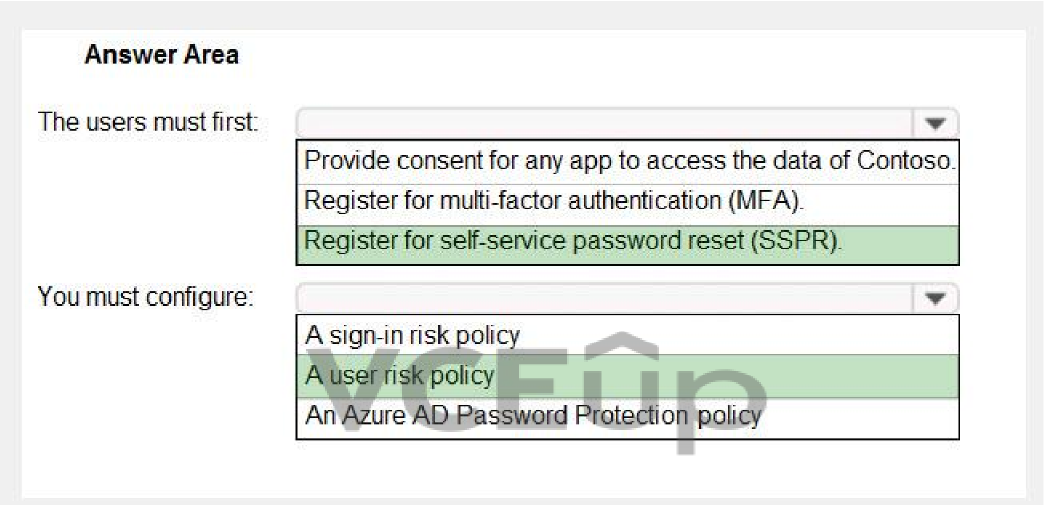
The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- Register for self-service password reset (SSPR).

You must configure:

- A sign-in risk policy
- A user risk policy
- An Azure AD Password Protection policy

Correct Answer:



Answer Area

The users must first:

- Provide consent for any app to access the data of Contoso.
- Register for multi-factor authentication (MFA).
- [✓ Register for self-service password reset (SSPR).]

You must configure:

- A sign-in risk policy
- [✓ A user risk policy]
- An Azure AD Password Protection policy

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/identity-protection/concept-identity-protection-policies

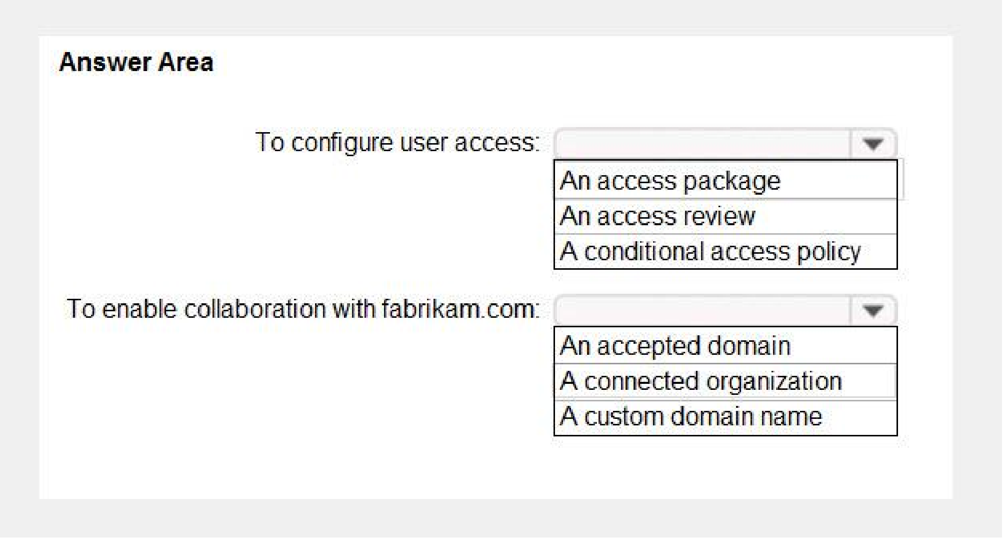
QUESTION 9
HOTSPOT

You need to implement the planned changes and technical requirements for the marketing department.

What should you do? To answer, select the appropriate options in the answer area.

NOTE: Each correct selection is worth one point.

Hot Area:



Answer Area

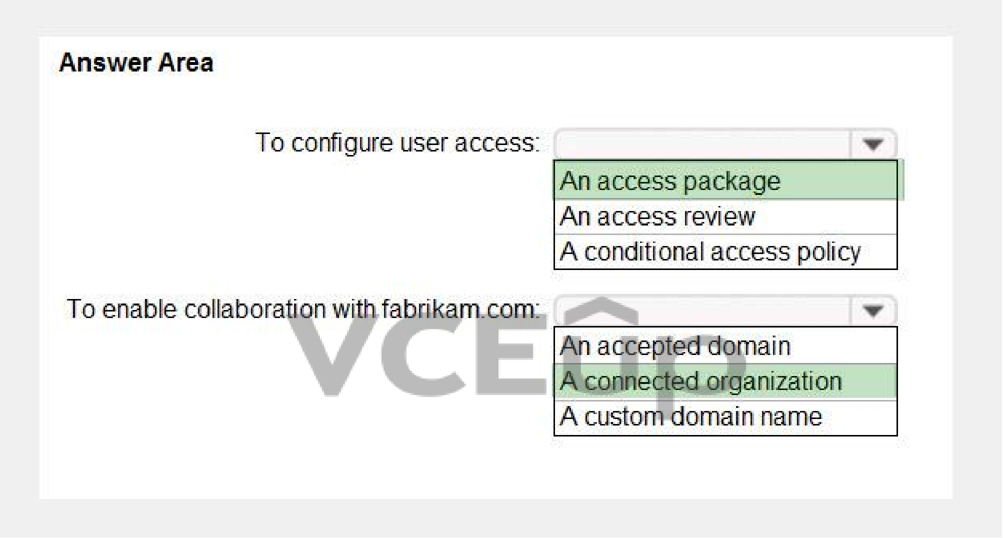
To configure user access:

- An access package
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:

- An accepted domain
- A connected organization
- A custom domain name

Correct Answer:



Answer Area

To configure user access:

- [✓ An access package]
- An access review
- A conditional access policy

To enable collaboration with fabrikam.com:

- An accepted domain
- [✓ A connected organization]
- A custom domain name

Section: (none)
Explanation

Explanation/Reference:
Reference:
https://docs.microsoft.com/en-us/azure/active-directory/governance/entitlement-management-organization